# This Page Is Inserted by IFW Operations and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents will not correct images, please do not report the images to the Image Problems Mailbox.

Web Account

O- Access the IEEE Member Digital Library

IEEE HOME | SEARCH IEEE | SHOP | WEB ACCOUNT | CONTACT IEEE



Publications/Services Standards Conferences Careers/Jobs Welcome **United States Patent and Trademark Office** » Se Quick Links - - - - -FAQ Terms IEEE Peer Review Welcome to IEEE Xplore® Your search matched 0 of 1015452 documents. O- Home A maximum of 500 results are displayed, 15 to a page, sorted by Relevance - What Can Descending order. I Access? O- Log-out **Refine This Search:** You may refine your search by editing the current search expression or enteri **Tables of Contents** new one in the text box. — Journals Search (network <near/1> security) <and> (finite <near/1> s & Magazines Check to search within this result set )- Conference **Proceedings Results Key:** ( )- Standards JNL = Journal or Magazine CNF = Conference STD = Standard Search O- By Author O- Basic Results: Advanced No documents matched your query. Member Services O Join IEEE O- Establish IEEE

Home | Log-out | Journals | Conference Proceedings | Standards | Search by Author | Basic Search | Advanced Search | Join IEEE | Web Account |
New this week | OPAC Linking Information | Your Feedback | Technical Support | Email Alerting | No Robots Please | Release Notes | IEEE Online
Publications | Help | FAQ | Terms | Back to Top

Copyright © 2004 IEEE — All rights reserved

O- Access the IEEE Member Digital Library

IEEE HOME | SEARCH IEEE | SHOP | WEB ACCOUNT | CONTACT IEEE



Publications/Services Standards Conferences Careers/Jobs Welcome **United States Patent and Trademark Office** » Se. Quiek Links Help FAQ Terms IEEE Peer Review Welcome to IEEE Xplore® Your search matched 0 of 1015452 documents. O- Home A maximum of 500 results are displayed, 15 to a page, sorted by Relevance — What Can **Descending** order. I Access? O- Log-out **Refine This Search:** You may refine your search by editing the current search expression or enteri **Tables of Contents** new one in the text box. — Journals (network <near/1> security) <and> (finite <near/1> s Search & Magazines Mark to search within this result set O- Conference **Proceedings Results Key:** O- Standards JNL = Journal or Magazine CNF = Conference STD = Standard Search C By Author O- Basic **Results:** No documents matched your query. — Advanced Member Services O- Establish IEEE Web Account

Home | Log-out | Journals | Conference Proceedings | Standards | Search by Author | Basic Search | Advanced Search | Join IEEE | Web Account |
New this week | OPAC Linking Information | Your Feedback | Technical Support | Email Alerting | No Robots Please | Release Notes | IEEE Online
Publications | Help | FAQ | Terms | Back to Top

Copyright © 2004 IEEE — All rights reserved



News Froogle New! <u>Images</u> Groups more »

"network security" "finite state machine" his



**Advanced Search** 

Web Results 1 - 10 of about 146 for "network security" "finite state machine" history length. (0.23 seconds

## FedCIRC Advisory FA-2000-21 Denial-of-Service

Vulnerabilities in ...

... A complete revision history is at the end ... implement the states of the TCP finite state machine. ... via various computer- and networksecurity related newsgroups ... www2.fedcirc.gov/advisories/FA-2000-21.html - 15k - Cached -Similar pages

Sponsored Links

**Network Security Papers** Free Reports & White Papers on the Latest Network Security Technology www.bitpipe.com

See your message here...

### CERT Advisory CA-2000-21

... implement the states of the TCP finite state machine. ... Revision History Nov 30, 2000: Initial ... re available for assignment: Network Security, Consulting, Server ... www.cotse.com/mailing-lists/cert/2000/0027.html - 64k - Cached - Similar pages

### APPENDIX B: Knowledge Areas of the IT Field

... Encryption and Computer & Network Security. X. ... Finite-state machine models Machine level representation of data ... History of computing Social contexts of computing ...

cne.gmu.edu/pjd/UAE/matrix.htm - 101k - Cached - Similar pages

### [PDF] APPENDIX B Knowledge Areas of the IT Field

File Format: PDF/Adobe Acrobat - View as HTML

... arithmetic Error propagation Abstraction Finite-state machine models Machine ... in this case.) History of computing ... theorem Finite word length effects Fourier and ... cne.gmu.edu/pjd/UAE/bodyofknowledge.pdf - Similar pages

#### [PDF] State-Machine Modelling in the DOVE System

File Format: PDF/Adobe Acrobat - View as HTML

... His research interests include computer network security, formal methods ... known in the literature as a "finite state machine". ... and a proof history which can ... www.dsto.defence.gov.au/isl/dove/Docs/theory.pdf - Similar pages

## [PDF] A Tool of Analysis and Implementation of Security Protocols on ...

File Format: PDF/Adobe Acrobat - View as HTML

... allow you to derive the finite state machine that constitutes ... ks,a]" of the Messages History shown in ... W. "Cryptography and Network Security: Principles and ... pegaso.ls.fi.upm.es/~Imengual/articulos/art 24.pdf - Similar pages

## Department of Electronics and Electrical Communication Engineering ...

... and latches, shifters, counters, finite state machine - state transition ... to finite register length effects on ... EC 61408 Communication and Network Security (3-0 ... www.ecdept.iitkgp.ernet.in/academics/btsylnewpg1.htm - 38k - Cached - Similar pages

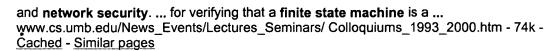
## [PDF] Active Systems Management: The Evolution of Firewalls

File Format: PDF/Adobe Acrobat - View as HTML

... A fundamental fact in computer and network security is that ... But as in the history of warfare, changes in ... Once the finite state machine is well defined, we must ... www.cs.umd.edu/~waa/pubs/asm-firewall.pdf - Similar pages

## UMASS Boston Department of Computer Science

... sciences, including its content, history, and applications. ... focus will be on computer



Proceedings of the 8th USENIX Security Symposium, August 23-36 ... ... C++ class simulates an extended finite state machine for matching ... matched an input event history that took ... Guha and B. Mukherjee, Network Security via

www.usenix.org/publications/library/proceedings/ sec99/full papers/sekar/sekar html/ -91k - Cached - Similar pages

## Gooooooogle >

1 2 3 4 5 6 7 8 9 10 Result Page:

"network security" "finite state ma

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Solutions - Business Solutions - About Google

©2004 Google



Web Images Groups News Froogle Newl more »

"network security" "state machines"

Search

Advanced Search Preferences

Web

Results 1 - 10 of about 1,900 for "network security" "state machines". (0.21 seconds)

## [PDF] Extensible Network Security Device Built with the Amplify Solution

File Format: PDF/Adobe Acrobat - <u>View as HTML</u> ... I/O pins constrainted Boundry I/O pins constrained Finite **state** machines generated in ... device extracted from database New, Customized **Network Security** Device: 9 ...

www.synplicity.com/literature/syndicated/ pdf/extensible\_v3\_i3.pdf - Similar pages

Sponsored Links

Network Security Papers
Free Reports & White Papers on the
Latest Network Security Technology
www.bitpipe.com

See your message here...

### Security Threat Management & Security Event Management

... by the state changes in the security correlation server's finite **state machines**). ... Threat Manager for its ability to view our **network security** systems and ... www.open.com/products/threatmanager/ STM2\_Architecture.shtml - 31k - Apr 1, 2004 - Cached - Similar pages

#### **Network Security**

... B. Security Protocols for **Network Security**. C. Need for Verifying Security Protocols. II. ... Protocols. 1. Use of methods based on **State Machines**. ... www.cs.fsu.edu/~yasinsac/ns04/Paper\_outline.htm - 21k - <u>Cached</u> - <u>Similar pages</u>

### **Corporate Communications Courses**

... CONTENTS **Network security** architectures : - Security architectures using network techniques like ... formal definition techniques, finite **state machines**, petri nets ... www.eurecom.fr/Curriculum/Teaching/ corporatecourses.html - 15k - <u>Cached</u> - Similar pages

#### Wireless LAN Security Site

... had only just gotten underway at the time that the IEEE 802.1X standard was approved, 802.1X does not describe how the 802.1X and 802.11 **state machines** are to ...

www.drizzle.com/~aboba/IEEE/ - 42k - Apr 1, 2004 - Cached - Similar pages

## Meetinghouse Data Communications: Securing the Mobile Network

... to the AEGIS Authenticator Toolkit library where the **state machines** act upon them ... Kevin Gagnon, a veteran of the **network security** industry and Meetinghouse's ... www.mtghouse.com/products/aegisskd/index.shtml - 37k - Apr 1, 2004 - <u>Cached - Similar pages</u>

### Meetinghouse Data Communications: Securing the Mobile Network

... Because the 802.1X **state machines** are completely insulated from the actual ... Kevin Gagnon, a veteran of the **network security** industry and Meetinghouse's Product ... www.mtghouse.com/products/aegisskd/ features/index.shtml - 34k - <u>Cached</u> - Similar pages

[ More results from www.mtghouse.com ]

#### Hardware holds value for classifying packets

... **Network security** has become increasingly important as a way to protect the ... the growing value of hardware, including programmable **state machines** and discrete ... www.eetimes.com/ printableArticle?doc\_id=OEG20031125S0046 - 8k - <u>Cached</u> - <u>Similar pages</u>

Intel(R) Networking & Communications - Network Associates, Inc.\* ... In theory, network security is simple: develop systems that can intelligently ... allows developers to build application logic using state machines and literally ... developer.intel.com/design/network/ casestudies/netassoc.htm - 47k - Cached -Similar pages

WPI's Department of Continuing Education introduces December ... ... WPI's computer and network security seminar will cover the following ... Access Controls; Computer Security Models (Bell-LaPadula, state machines, BLP significance ... www.wpi.edu/News/TechNews/article.php?id=149 - 12k - Cached - Similar pages

Gooooooogle ▶

Result Page: 1 2 3 4 5 6 7 8 9 10

"network security" "state machine Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Solutions - Business Solutions - About Google

©2004 Google



Froogle<sup>New!</sup> Web **Images** Groups News more »

"audit file" (netowrk OR networking)

Search

Advanced Search **Preferences** 

Results 1 - 10 of about 619 for "audit file" (netowrk OR networking). (0.28 seconds)

Did you mean: "audit file" (network OR networking)

Step-By-Step: How to audit file and folder access to improve ...

... Enabling auditing Before you can audit file and folder access, you must enable ... Cisco Storage Networking Blueprint Cisco Systems | PDF; Cisco Systems Intelligent ...

techrepublic.com.com/5100-6270-5034308-1-1.html - 33k - Cached -Similar pages

#### audit File for BNU

... This file is part of the Basic Networking Utilities Program (BNU) in BOS Extensions 1. Files. /var/spool/uucp/.Admin/audit, Specifies the path of the

www.unet.univie.ac.at/aix/files/aixfiles/audit BNU.htm - 4k - Cached -Similar pages

Sponsored Links

#### **FileAudit**

Monitor access to your most sensitive files. Free Trial. www.softwareshelf.com

#### Hardware Audit

Audit your computer network and detect all hardware components. www.PCinfo.biz

See your message here...

Files Topics: Operating System Files

... used by HCON. Basic Networking Utilities (BNU) Files. audit File for BNU, Contains debug messages from the uucico daemon. Command (C ... www.unet.univie.ac.at/aix/aixgen/ wbinfnav/OpSysFiles.htm - 28k - Cached -Similar pages

[ More results from www.unet.univie.ac.at ]

Byte and Switch - The Global Site For Storage Networking

... (Nasdag: FALC - message board) to develop a special script to allow WorldCare to audit file movement on the ... Discuss this story >. Storage Networking Marketplace ... www.byteandswitch.com/document.asp?doc id=25078 - 49k - Cached - Similar pages

#### Router Security Audit Logs-Cisco IOS Software Releases 12.2 S ...

Area Navigation Business Industries & Solutions. ... message, and all syslog message are kept in the audit file, which is ... www.cisco.com/en/US/products/sw/iosswrel/ps1838/

products feature guide09186a00801afa4f.html - 101k - Cached - Similar pages

#### [PDF] Router Security Audit Logs

File Format: PDF/Adobe Acrobat - View as HTML

... Command Description audit filesize Changes the size of the audit file. ... Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network ... www.cisco.com/univercd/cc/td/doc/product/software/ ios122s/122snwft/release/122s18/gtaudlog.pdf - Similar pages

[ More results from www.cisco.com ]

#### rpoci The CharterGroup

File Format: Microsoft Word 2000 - View as HTML

... Network. THE BENEFITS OF NETWORKING INTERACTION. We are working with members to develop the Sole Practitioner Network. ... Price per pack. Audit file. £ 18.00.

www.chartergroup.co.uk/uploadable\_docs/ the\_chartergroup\_services.doc -Similar pages

Internet & Networking Networking Monitoring Free & Shareware ...

... Networking. ... Audit last user and change dates and keep history into files comments property field Put audit file modifications in Windows 2000 and Macintosh ... www.ezgoal.com/ channels/internet/c.asp? cid=199571&p=4&o=&s=&l=&Downloads=Internet+Softwar - 76k - Cached -Similar pages

**Batch Degree Audit Control Sheet** 

... If record to read from requirements file not modified, the default (%COM) record will be used. Build Audit File for Web. Y blank. Y = Yes blank = No. Comments. ... www.bgsu.edu/offices/its/forms/batch-degree-audit.html - 65k - Cached - Similar pages

<u>Langara College - Continuing Studies Course Descriptions</u> ... Upon completion of the year-end audit file, it will be reviewed by a ... Review the underlying telecommunications, data communications, and networking technologies ... www.langara.bc.ca/cs/programs/AINF.html - 24k - Apr 1, 2004 - Cached - Similar pages

Did you mean to search for: "audit file" (network OR networking)

Gooooooogle ▶

1 2 3 4 5 6 7 8 9 10 Result Page: Next

"audit file" (netowrk OR networkir Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Solutions - Business Solutions - About Google

©2004 Google



Web Images Groups News Froogle New! more »

"network security" "finite state machine"

Search

Advanced Search Preferences

Web

Results 1 - 10 of about 784 for "network security" "finite state machine". (0.09 seconds)

## [PDF] The Design and Implementation of Network Intrusion Detection ...

File Format: PDF/Adobe Acrobat - View as HTML

... Network security seems to become much more important in recent years ... intrusion detection system using XML [XML00] and finite state machine technologies, which ...

hcs.nctu.edu.tw/second/second.pdf - Similar pages

Sponsored Links

Network Security Papers
Free Reports & White Papers on the
Latest Network Security Technology
www.bitpipe.com

See your message here...

#### NerveCenter 3.8 Announcement

... (Open), the leader in **network security** management software ... Based on **finite state machine** theory and extensible using PERL, the industry-standard scripting ... www.open.com/news/021202.shtml - 24k - <u>Cached</u> - <u>Similar pages</u>

### Network Security Laboratories, Inc. (NSLI), Bethesda, MD

... UNIX kernels, TCP/IP internals, O/S and **network security** products, Internet e ... Built the first complete **finite state machine** (FSM) characterization and formal ... www.nsli.com/resume.htm - 20k - Cached - Similar pages

### Hardware holds value for classifying packets

... **Network security** has become increasingly important as a way to protect the ... graph and using the software implementation of a **finite-state machine** to locate the ... www.eetimes.com/ printableArticle?doc\_id=OEG20031125S0046 - 8k - <u>Cached</u> - Similar pages

#### Resume

... My research interests lie in the area of **network security** for wireless ... Other interests include fault detection, **Finite State Machine** modeling and Hidden Markov ... www.glue.umd.edu/~svetlana/resume.html - 18k - Cached - Similar pages

#### Research

My research interests lie in the area of **network security** with emphasis on ... of buffer overflow attacks and we developed **Finite State Machine** models for various ... www.glue.umd.edu/~svetlana/research.html - 9k - Cached - Similar pages

#### research

... Network Security. ... In the first project we develop a finite-state machine based approach for the formal verification of various authentication protocols that has ... engr.smu.edu/~nair/research.html - 4k - <u>Cached</u> - <u>Similar pages</u>

#### CSE 398: Network Programming

... transmission (stop-and-wait, sliding window) 02/24: Finite state machine; Go-back ... MPEG) 03/26: Multimedia networking applications, ARP Network Security (2 hours ... www.cse.lehigh.edu/~cheng/Teaching/ CSE398/schedule.html - 6k - Cached - Similar pages

### [poc] Programme Specification

File Format: Microsoft Word 2000 - View as HTML

... network security requirements and implement appropriate defences;; design and implement assembly language programs;; design and implement a finite state machine;; ...

www.brunel.ac.uk/depts/ee/ugsylls/EE2073.doc - Similar pages

#### Fault-tolerant and Secure Communication

... Security: (i) Explore mechanisms/algorithms for identifying jammed or totally failed area in ... J. Xu, and RK lyer, "A Data-Driven Finite State Machine Model for ... www-rtsl.cs.uiuc.edu/muri/research/iyer.html - 9k - Cached - Similar pages

## Gooooooogle >

Result Page: 1 2 3 4 5 6 7 8 9 10 Nex

"network security" "finite state ma Sea

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

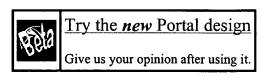
Google Home - Advertising Solutions - Business Solutions - About Google

©2004 Google



> home : > about : > feedback : > login

US Patent & Trademark Office



## Search Results

Search Results for: [(finite AND state AND machine) AND (network AND security) <AND>(meta\_published\_date <= 10-01-2000 )]
Found 504 of 698 searched out of 129,763.

Warning: Maximum result set of 200 exceeded. Consider refining.

Search within I	Results				
	·		Go	> Advanced Search	:
> Search Help/Tips					
Sort by: Title	Publication	Publication Date	Score		
Results 1 - 20 of	200 shor Prev Page	t listing 1 2 3 4 5 6	7 8 9	Next Page	

SAFKASI: a security mechanism for language-based systems

95%

Dan S. Wallach , Andrew W. Appel , Edward W. Felten

**ACM Transactions on Software Engineering and Methodology (TOSEM)** October 2000

Volume 9 Issue 4

In order to run untrusted code in the same process as trusted code, there must be a mechanism to allow dangerous calls to determine if their caller is authorized to exercise the privilege of using the dangerous routine. Java systems have adopted a technique called stack inspection to address this concern. But its original definition, in terms of searching stack frames, had an unclear relationship to the actual achievement of security, overconstrained the implementation of a Java system, lim ...

2 An efficient and lightweight embedded Web server for Web-based network element management

88%

Hong-Taek Ju , Mi-Joung Choi , James W. Hong

**International Journal of Network Management** September 2000 Volume 10 Issue 5

An Embedded Web Server & lpar; EWS) is a Web server which runs on an embedded system with limited computing resources to serve embedded Web documents to a Web browser. By embedding a Web server into a network device, it is possible to provide a Web‐ based management user interface, which are user‐ friendly, inexpensive, cross‐ platform, and network‐ ready. This article explores the topic of an efficient and lightweight embedded Web server for Web‐ based netw ...

**3** Performance analysis of MD5

88%



Joseph D. Touch

ACM SIGCOMM Computer Communication Review, Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication October 1995

Volume 25 Issue 4

MD5 is an authentication algorithm proposed as the required implementation of the authentication option in IPv6. This paper presents an analysis of the speed at which MD5 can be implemented in software and hardware, and discusses whether its use interferes with high bandwidth networking. The analysis indicates that MD5 software currently runs at 85 Mbps on a 190 Mhz RISC architecture, a rate that cannot be improved more than 20-40%. Because MD5 processes the entire body of a packet, this data ra ...

4 Strategic directions in research in theory of computing

88%

Michael C. Loui

ACM Computing Surveys (CSUR) December 1996

Volume 28 Issue 4

A type system for expressive security policies

87%

David Walker

Proceedings of the 27th ACM SIGPLAN-SIGACT symposium on Principles of programming languages January 2000

Certified code is a general mechanism for enforcing security properties. In this paradigm, untrusted mobile code carries annotations that allow a host to verify its trustworthiness. Before running the agent, the host checks the annotations and proves that they imply the host's security policy. Despite the flexibility of this scheme, so far, compilers that generate certified code have focused on simple type safety properties rather than more general security properties.

6 Temporal sequence learning and data reduction for anomaly detection Terran Lane , Carla E. Brodley

87%

87%

ACM Transactions on Information and System Security (TISSEC) August 1999 Volume 2 Issue 3

The anomaly-detection problem can be formulated as one of learning to characterize the behaviors of an individual, system, or network in terms of temporal sequences of discrete data. We present an approach on the basis of instance-based learning (IBL) techniques. To cast the anomaly-detection task in an IBL framework, we employ an approach that transforms temporal sequences of discrete, unordered observations into a metric space via a similarity measure that encodes intra-attribute depende ...

**7** PELLPACK: a problem-solving environment for PDE-based applications on multicomputer platforms

E. N. Houstis , J. R. Rice , S. Weerawarana , A. C. Catlin , P. Papachiou , K.-Y. Wang , M. Gaitatzes

ACM Transactions on Mathematical Software (TOMS) March 1998 Volume 24 Issue 1

The article presents the software architecture and implementation of the problemsolving environment (PSE) PELLPACK for modeling physical objects described by partial differential equations (PDEs). The scope of this PSE is broad, as PELLPACK incorporates many PDE solving systems, and some of these, in turn, include several specific PDE solving methods. Its coverage for 1D, 2D. and 3D elliptic or parabolic problems is quite broad, and it handles some hyperbolic problems, Since a PSE should p ...

**8** Curriculum recommendations for undergraduate programs in information systems

85%

J. Daniel Couger

**Communications of the ACM** December 1973

Volume 16 Issue 12

9 Distributed systems - programming and management: On remote **∤** procedure call

85%

Patrícia Gomes Soares

Proceedings of the 1992 conference of the Centre for Advanced Studies on Collaborative research - Volume 2 November 1992

The Remote Procedure Call (RPC) paradigm is reviewed. The concept is described, along with the backbone structure of the mechanisms that support it. An overview of works in supporting these mechanisms is discussed. Extensions to the paradigm that have been proposed to enlarge its suitability, are studied. The main contributions of this paper are a standard view and classification of RPC mechanisms according to different perspectives, and a snapshot of the paradigm in use today and of goals for t ...

**10** The development and proof of a formal specification for a multilevel

85%

ৰী secure system

Janice I. Glasgow , Glenn H. MacEwen

ACM Transactions on Computer Systems (TOCS) March 1987

Volume 5 Issue 2

This paper describes current work on the design and specification of a multilevel secure distributed system called SNet. It discusses security models in general, the various problems of information flows in SNet, and the abstract and concrete security model components for SNet. It also introduces Lucid as a language for specifying distributed systems. The model components are expressed in Lucid; these Lucid partial specifications are shown to be correct with respect to the formal model, and ...

**11** Using a coordination language to specify and analyze systems **A** containing mobile components

85%

P. Ciancarini , F. Franzé , C. Mascolo

ACM Transactions on Software Engineering and Methodology (TOSEM) April 2000 Volume 9 Issue 2

New computing paradigms for network-aware applications need specification languages able to deal with the features of mobile code-based systems. A coordination language provides a formal framework in which the interaction of active entities can be expressed. A coordination language deals with the creation and destruction of code or complex agents, their communication activites, as well as their distribution and mobility in space. We show how the coordination language PoliS offers a flexible ...

**12** Computing as a discipline

84%

D. E. Comer, David Gries, Michael C. Mulder, Allen Tucker, A. Joe Turner, Paul R. Youna

**Communications of the ACM** February 1989

Volume 32 Issue 1

The final report of the Task Force on the Core of Computer Science presents a new intellectual framework for the discipline of computing and a new basis for computing curricula. This report has been endorsed and approved for release by the ACM



Education Board.

13 Curriculum recommendations for graduate professional programs in

84%

ৰী information systems

Communications of the ACM May 1972

Volume 15 Issue 5

14 Curriculum '78: recommendations for the undergraduate program in

83%

ब्री computer science— a report of the ACM curriculum committee on computer science

Richard H. Austing, Bruce H. Barnes, Della T. Bonnette, Gerald L. Engel, Gordon Stokes Communications of the ACM March 1979

Volume 22 Issue 3

Contained in this report are the recommendations for the undergraduate degree program in Computer Science of the Curriculum Committee on Computer Science (C3S) of the Association for Computing Machinery (ACM). The core curriculum common to all computer science undergraduate programs is presented in terms of elementary level topics and courses, and intermediate level courses. Elective courses, used to round out an undergraduate program, are then discussed, and ...

15 Formal methods: state of the art and future directions

83%

Edmund M. Clarke, Jeannette M. Wing

ACM Computing Surveys (CSUR) December 1996

Volume 28 Issue 4

16 Anonymous credit cards

83%

Steven H. Low , Sanjoy Paul , Nicholas F. Maxemchuk Proceedings of the 2nd ACM Conference on Computer and communications security November 1994

This paper describes a communications networking technique for funds transfer which combines the privacy of cash transactions with the security, record-keeping and charging mechanisms of credit cards. The scheme uses a communications network and cryptographic protocols to separate information. The company that extends credit to the individual and collects the bill does not have access to the specific purchases, and the shop that sells the merchandise is convinced that it will be paid withou ...

17 Proofs that yield nothing but their validity or all languages in NP have

बो zero-knowledge proof systems

Oded Goldreich , Silvio Micali , Avi Wigderson

Journal of the ACM (JACM) July 1991

Volume 38 Issue 3

18 Improving the aircraft design process using Web-based modeling and

83%

83%

ৰী simulation

John A. Reed , Gregory J. Follen , Abdollah A. Afjeh

ACM Transactions on Modeling and Computer Simulation (TOMACS) January 2000 Volume 10 Issue 1

Designing and developing new aircraft systems is time-consuming and expensive. Computational simulation is a promising means for reducing design cycle times, but requires a flexible software environment capable of integrating advanced



multidisciplinary and multifidelity analysis methods, dynamically managing data across heterogeneous computing platforms, and distributing computationally complex tasks. Web-based simulation, with its emphasis on collaborative composition of simulation models, ...

19 Fast detection of communication patterns in distributed executions

82%



Thomas Kunz , Michiel F. H. Seuren

Proceedings of the 1997 conference of the Centre for Advanced Studies on Collaborative research November 1997

Understanding distributed applications is a tedious and difficult task. Visualizations based on process-time diagrams are often used to obtain a better understanding of the execution of the application. The visualization tool we use is Poet, an event tracer developed at the University of Waterloo. However, these diagrams are often very complex and do not provide the user with the desired overview of the application. In our experience, such tools display repeated occurrences of non-trivial commun ...

20 m-EVES: A tool for verifying software

82%

🛕 D. Craigen , S. Kromodimoeljo , I. Meisels , A. Neilson , B. Pase , M. Saaltink Proceedings of the 10th international conference on Software engineering April 1988

This paper describes the development of a new tool for formally verifying software. The tool is called m-EVES and consists of a new language, called m-Verdi, for implementing and specifying software; a new logic, which has been proven sound; and a new theorem prover, called m-NEVER, which integrates many state-of-the-art techniques drawn from the theorem proving literature. Two simple examples are used to present the fundamental ideas embodied within the system.

Results 1 - 20 of 200

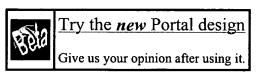
short listing



The ACM Portal is published by the Association for Computing Machinery. Copyright © 2004 ACM, Inc.



> about > feedback **US Patent & Trademark Office** 



### Search Results

Search Results for: [(finite AND state AND machine) AND (network AND

security) ]

Found **698** of **129,763 searched**.

Warning: Maximum result set of 200 exceeded. Consider refining.

Search within Results GO > Advanced Search > Search Help/Tips

Sort by:	Title	Publica	ition	Pı	ıbli	icat	ion	Da	ite	S	cor	e				
Results 1	- 20 of	200	short Prev Page				4	5	6	7	8	9	10	C> Next Page		

Real-time protocol analysis for detecting link-state routing protocol attacks

98%

Ho-Yen Chang, S. Felix Wu, Y. Frank Jou

ACM Transactions on Information and System Security (TISSEC) February 2001 Volume 4 Issue 1

A real-time knowledge-based network intrusion-detection model for a link-state routing protocol is presented for the OSPF protocol. This model includes three layers: a data process layer to parse packets and dispatch data; and event abstractor to abstract predefined real-time events for the link-state routing protocol; and an extended timed finite state machine to express the real-time behavior of the protocol engine and to ...

SAFKASI: a security mechanism for language-based systems Dan S. Wallach , Andrew W. Appel , Edward W. Felten

95%

ACM Transactions on Software Engineering and Methodology (TOSEM) October 2000

Volume 9 Issue 4

In order to run untrusted code in the same process as trusted code, there must be a mechanism to allow dangerous calls to determine if their caller is authorized to exercise the privilege of using the dangerous routine. Java systems have adopted a technique called stack inspection to address this concern. But its original definition, in terms of searching stack frames, had an unclear relationship to the actual achievement of security, overconstrained the implementation of a Java system, lim ...

Computing curricula 2001

94%

Journal on Educational Resources in Computing (JERIC) September 2001





Termination in language-based systems

89%



Algis Rudys , Dan S. Wallach

ACM Transactions on Information and System Security (TISSEC) May 2002 Volume 5 Issue 2

Language run-time systems are increasingly being embedded in systems to support run-time extensibility via mobile code. Such systems raise a number of concerns when the code running in such systems is potentially buggy or untrusted. Although sophisticated access controls have been designed for mobile code and are shipping as part of commercial systems such as Java, there is no support for terminating mobile code short of terminating the entire language run-time. This article presents a c ...

Simple, state-based approaches to program-based anomaly detection C. C. Michael , Anup Ghosh

88%

ACM Transactions on Information and System Security (TISSEC) August 2002 Volume 5 Issue 3

This article describes variants of two state-based intrusion detection algorithms from Michael and Ghosh [2000] and Ghosh et al. [2000], and gives experimental results on their performance. The algorithms detect anomalies in execution audit data. One is a simply constructed finite-state machine, and the other two monitor statistical deviations from normal program behavior. The performance of these algorithms is evaluated as a function of the amount of available training data, and they are compar ...

Session 1: creative mathematics: Model-Carrying Code (MCC): a new প্রী paradigm for mobile-code security

88%

R. Sekar, C. R. Ramakrishnan, I. V. Ramakrishnan, S. A. Smolka

Proceedings of the 2001 workshop on New security paradigms September 2001 A new approach for ensuring the security of mobile code is proposed. Our approach enables a mobile-code consumer to understand and formally reason about what a piece of mobile code can do; check if the actions of the code are compatible with his/her security policies; and, if so, execute the code. The compatibility-checking process is automated, but if there are conflicts, consumers have the opportunity to refine their policies, taking into account the functionality provided by the mobile code.

Intrusion detection: Specification-based anomaly detection: a new ৰী approach for detecting network intrusions

88%

R. Sekar , A. Gupta , J. Frullo , T. Shanbhag , A. Tiwari , H. Yang , S. Zhou Proceedings of the 9th ACM conference on Computer and communications security November 2002

Unlike signature or misuse based intrusion detection techniques, anomaly detection is capable of detecting novel attacks. However, the use of anomaly detection in practice is hampered by a high rate of false alarms. Specification-based techniques have been shown to produce a low rate of false alarms, but are not as effective as anomaly detection in detecting novel attacks, especially when it comes to network probing and denial-of-service attacks. This paper presents a new approach that combines ...

An efficient and lightweight embedded Web server for Web-based

88%



ৰী network element management

Hong-Taek Ju, Mi-Joung Choi, James W. Hong International Journal of Network Management September 2000

#### Volume 10 Issue 5

An Embedded Web Server ( EWS) is a Web server which runs on an embedded system with limited computing resources to serve embedded Web documents to a Web browser. By embedding a Web server into a network device, it is possible to provide a Web‐ based management user interface, which are user‐ friendly, inexpensive, cross‐ platform, and network‐ ready. This article explores the topic of an efficient and lightweight embedded Web server for Web‐ based netw ...

9 Performance analysis of MD5

88%



Joseph D. Touch

ACM SIGCOMM Computer Communication Review, Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication October 1995

Volume 25 Issue 4

MD5 is an authentication algorithm proposed as the required implementation of the authentication option in IPv6. This paper presents an analysis of the speed at which MD5 can be implemented in software and hardware, and discusses whether its use interferes with high bandwidth networking. The analysis indicates that MD5 software currently runs at 85 Mbps on a 190 Mhz RISC architecture, a rate that cannot be improved more than 20-40%. Because MD5 processes the entire body of a packet, this data ra ...

**10** Strategic directions in research in theory of computing

88%



Michael C. Loui

ACM Computing Surveys (CSUR) December 1996

Volume 28 Issue 4

**11** A type system for expressive security policies

87%



David Walker

Proceedings of the 27th ACM SIGPLAN-SIGACT symposium on Principles of programming languages January 2000

Certified code is a general mechanism for enforcing security properties. In this paradigm, untrusted mobile code carries annotations that allow a host to verify its trustworthiness. Before running the agent, the host checks the annotations and proves that they imply the host's security policy. Despite the flexibility of this scheme, so far, compilers that generate certified code have focused on simple type safety properties rather than more general security properties.

12 Temporal sequence learning and data reduction for anomaly detection Terran Lane , Carla E. Brodley

87%



ACM Transactions on Information and System Security (TISSEC) August 1999 Volume 2 Issue 3

The anomaly-detection problem can be formulated as one of learning to characterize the behaviors of an individual, system, or network in terms of temporal sequences of discrete data. We present an approach on the basis of instance-based learning (IBL) techniques. To cast the anomaly-detection task in an IBL framework, we employ an approach that transforms temporal sequences of discrete, unordered observations into a metric space via a similarity measure that encodes intra-attribute depende ...

**13** PELLPACK: a problem-solving environment for PDE-based applications বী on multicomputer platforms

87%







E. N. Houstis, J. R. Rice, S. Weerawarana, A. C. Catlin, P. Papachiou, K.-Y. Wang, M. Gaitatzes

ACM Transactions on Mathematical Software (TOMS) March 1998 Volume 24 Issue 1

The article presents the software architecture and implementation of the problemsolving environment (PSE) PELLPACK for modeling physical objects described by partial differential equations (PDEs). The scope of this PSE is broad, as PELLPACK incorporates many PDE solving systems, and some of these, in turn, include several specific PDE solving methods. Its coverage for 1D, 2D. and 3D elliptic or parabolic problems is quite broad, and it handles some hyperbolic problems, Since a PSE should

14 Session 2: secure Web services: Designing a distributed access control nprocessor for network services on the Web

85%

Reiner Kraft

Proceedings of the 2002 ACM workshop on XML security November 2002 The service oriented architecture (SOA) is gaining more momentum with the advent of network services on the Web. A programmable and machine accessible Web is the vision of many, and might represent a step towards the semantic Web. However, security is a crucial requirement for the serious usage and adoption of the Web services technology. This paper enumerates design goals for an access control model for Web services. It then introduces an abstract general model for Web services components, along ...

15 Curriculum recommendations for undergraduate programs in

85%

information systems

J. Daniel Couger

Communications of the ACM December 1973

Volume 16 Issue 12

16 Distributed systems - programming and management: On remote

85%

ৰী procedure call

Patrícia Gomes Soares

Proceedings of the 1992 conference of the Centre for Advanced Studies on Collaborative research - Volume 2 November 1992

The Remote Procedure Call (RPC) paradigm is reviewed. The concept is described, along with the backbone structure of the mechanisms that support it. An overview of works in supporting these mechanisms is discussed. Extensions to the paradigm that have been proposed to enlarge its suitability, are studied. The main contributions of this paper are a standard view and classification of RPC mechanisms according to different perspectives, and a snapshot of the paradigm in use today and of goals for t ...

17 Survivability analysis of networked systems

85%

Somesh Jha , Jeannette M. Wing

Proceedings of the 23rd international conference on Software engineering July 2001

Survivability is the ability of a system to continue operating despite the presence of abnormal events such as failures and intrusions. Ensuring system survivability has increased in importance as critical infrastructures have become heavily dependent on computers. In this paper we present a systematic method for performing survivability analysis of networked systems. An architect injects failure and intrusion events into a





system model and then visualizes the effects of the injected event ...

18 An Internet multicast system for the stock market ACM Transactions on Computer Systems (TOCS) August 2001 85%

Volume 19 Issue 3

We are moving toward an international, 24-hour, distributed, electronic stock exchange. The exchange will use the global Internet, or internet technology. This system is a natural application of multicast because there are a large number of receivers that should receive the same information simultaneously. The data requirements for the stock exchange are discussed. The current multicast protocols lack the reliability, fairness, and scalability needed in this application. We describe a distr ...

19 The development and proof of a formal specification for a multilevel

85%

ৰী secure system

Janice I. Glasgow, Glenn H. MacEwen

ACM Transactions on Computer Systems (TOCS) March 1987

Volume 5 Issue 2

This paper describes current work on the design and specification of a multilevel secure distributed system called SNet. It discusses security models in general, the various problems of information flows in SNet, and the abstract and concrete security model components for SNet. It also introduces Lucid as a language for specifying distributed systems. The model components are expressed in Lucid; these Lucid partial specifications are shown to be correct with respect to the formal model, and ...

**2**0 Verifying security protocols as planning in logic programming

85%

🖈 Luigia Carlucci Aiello , Fabio Massacci

ACM Transactions on Computational Logic (TOCL) October 2001

Volume 2 Issue 4.

We illustrate ALSP (Action Language for Security Protocol), a declarative executable specification language for planning attacks to security protocols. ALSP is based on logic programming with negation as failure, and with stable model semantics. In ALSP we can give a declarative specification of a protocol with the natural semantics of send and receive actions which can be performed in parallel. By viewing a protocol trace as a plan to a ...

Results 1 - 20 of 200

short listing

Prev Page 1 5 7 8 9 10

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2004 ACM, Inc.





News Froogle New! **Images** Groups more »

"network security" "finite state machine" his

Search.

**Advanced Search** 

Web Results 1 - 10 of about 146 for "network security" "finite state machine" history length. (0.23 seconds

## FedCIRC Advisory FA-2000-21 Denial-of-Service

Vulnerabilities in ...

... A complete revision history is at the end ... implement the states of the TCP finite state machine ... via various computer- and networksecurity related newsgroups ... www2.fedcirc.gov/advisories/FA-2000-21.html - 15k - Cached -Similar pages

Sponsored Links

Network Security Papers Free Reports & White Papers on the Latest Network Security Technology www.bitpipe.com

See your message here...

## CERT Advisory CA-2000-21

... implement the states of the TCP finite state machine. ... Revision History Nov 30, 2000: Initial ... re available for assignment: Network Security, Consulting, Server ... www.cotse.com/mailing-lists/cert/2000/0027.html - 64k - Cached - Similar pages

#### APPENDIX B: Knowledge Areas of the IT Field

... Encryption and Computer & Network Security. X. ... Finite-state machine models Machine level representation of data ... History of computing Social contexts of computing ...

cne.gmu.edu/pjd/UAE/matrix.htm - 101k - Cached - Similar pages

### [PDF] APPENDIX B Knowledge Areas of the IT Field

File Format: PDF/Adobe Acrobat - View as HTML

... arithmetic Error propagation Abstraction Finite-state machine models Machine ... in this case.) History of computing ... theorem Finite word length effects Fourier and ... cne.gmu.edu/pjd/UAE/bodyofknowledge.pdf - Similar pages

#### [PDF] State-Machine Modelling in the DOVE System

File Format: PDF/Adobe Acrobat - View as HTML

... His research interests include computer network security, formal methods ... known in the literature as a "finite state machine". ... and a proof history which can ... www.dsto.defence.gov.au/isl/dove/Docs/theory.pdf - Similar pages

## [PDF] A Tool of Analysis and Implementation of Security Protocols on ...

File Format: PDF/Adobe Acrobat - View as HTML

... allow you to derive the finite state machine that constitutes ... ks,a]" of the Messages History shown in ... W. "Cryptography and Network Security: Principles and ... pegaso.ls.fi.upm.es/~lmengual/articulos/art 24.pdf - Similar pages

## Department of Electronics and Electrical Communication Engineering ...

... and latches, shifters, counters, finite state machine - state transition ... to finite register length effects on ... EC 61408 Communication and Network Security (3-0 ... www.ecdept.iitkgp.ernet.in/academics/btsylnewpg1.htm - 38k - Cached - Similar pages

## [PDF] Active Systems Management: The Evolution of Firewalls

File Format: PDF/Adobe Acrobat - View as HTML

... A fundamental fact in computer and network security is that ... But as in the history of warfare, changes in ... Once the finite state machine is well defined, we must ... www.cs.umd.edu/~waa/pubs/asm-firewall.pdf - Similar pages

## UMASS Boston Department of Computer Science

... sciences, including its content, history, and applications. ... focus will be on computer



and network security. ... for verifying that a finite state machine is a ... www.cs.umb.edu/News\_Events/Lectures\_Seminars/ Colloquiums\_1993\_2000.htm - 74k -Cached - Similar pages

Proceedings of the 8th USENIX Security Symposium, August 23-36 ... ... C++ class simulates an extended finite state machine for matching ... matched an input event history that took ... Guha and B. Mukherjee, Network Security via Reverse ...

www.usenix.org/publications/library/proceedings/ sec99/full papers/sekar/sekar html/ -91k - Cached - Similar pages

Gooooooogle >

Result Page: 1 2 3 4 5 6 7 8 9 10

"network security" "finite state ma

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Solutions - Business Solutions - About Google

©2004 Google

## **Network Security**

## Paper Outline

As part of the paper(s) required for the course, students will submit a one page proposed outline of their paper as scheduled on the course calendar. The outline should highlight the paper's topic and detail the approach the student will take in presenting the material. An average outline s provided below as a sample.

**Deadline for submission:** 

See the course calendar

Required Length:

One page

Format:

Outline

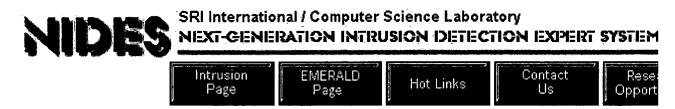
**Submission method**: Email. The subject of the email must be "Paper Outline". The outline will be within the body of the email. No attachments will be accepted.

Sample Outline: Paper Outline for "Impact of Protocol Interaction on Verifying Protocols".

- I.Introduction and Background
- A. Need for Network Security
- B. Security Protocols for Network Security
- C. Need for Verifying Security Protocols
- II. Verifying Security Protocols
- A. Testing of Security Protocols
- B. Application of Formal Methods to verify Security

#### **Protocols**

- 1. Use of methods based on State Machines
- 2. Use of methods based on Modal Logic
- C. Other Methods to verify Security Protocols
- III. Protocol Interaction
- A. What is Protocol Interaction?
- B. Why do Protocol Interactions Occur?
- C. Examples of Protocol Interactions
- D. Attacks based on Protocol Interactions
- IV. Impacts of Protocol Interaction
- A. Impact on the verification of Protocols
- B. Issues to be considered
- C. Design principles to be followed
- V. Conclusion
- VI.Bibliography



## Reports and Papers Available for Download (as of Jan. 19 1998)

## Please check this page again as new documents may be loaded late

## <CLICK TO RETURN>

Title	Authors	Data	Si
SAFEGUARD Final Report: Detecting Unusual Program Behavior Using the NIDES Statistical Component	Anderson, Valdes	12/95	77ր 183,2
NIDES: A Summary	Anderson, Frivold, Valdes	5/95	47ŗ 236,8
Detecting Unusual Program Behavior Using the Statistical Components of NIDES	Anderson, Lunt, Javits, Tamaru, Valdes	5/95	86r 2,151,
NIDES: Software Users Manual Beta-Update Release (GET IT!)	Anderson, Frivold, Tamaru, Valdes	12/94	316 4,232,
NIDES: Training Course Beta Release	Anderson, Frivold, Valdes	8/94	360 3,564,
NIDES Software Design, Product Specification, and Version  Description Documentation	Anderson, Frivold, Tamaru, Valdes	7/94	86r 321,9
Software Requirements Specification: Next-Generation Intrusion Detection Expert System	Lunt, Anderson	3/94	27; 53,3
Detecting Intruders in Computer Systems	Lunt	93	17բ 62,0։
The NIDES Statistical Component:  Description and Justification	Javits, Valdes	3/93	47 <sub>1</sub> 254,2

NIDES: System Design Document	Jagannathan, Lunt, Dodd, Anderson, Gilham, Jalali,Javits, Neumann, Tamaru, Valdes	3/93	74; 230,5
The NIDES Statistical Component:  Description and Justification	Javits, Valdes	3/93	47; 131,5
A Real-Time Intrusion Detection Expert System	Lunt, Tamaru, Gilham, Jagannathan, Jalali,Javitz Neumann, Valdes, Garvey	2/92	166 1,141,
The SRI IDES Statistical Anomaly Detector	Javits, Valdes	5/91	11 <u>;</u> 82,2
Automated Audit Trail Analysis and Intrusion Detection: A Survey	Lunt	10/88	17ր 57,7։
IDES: The Enhanced Prototype	Lunt, Lee Jagannathan, Listgarten, Edwards, Neumann, Javitz, Valdes	10/88	88ŗ 1,326,



Froogle<sup>New!</sup> <u>Images</u> **Groups** News more »

anderson lunt javitz "next generation intrusi

Search

Advanced Search **Preferences** 

Web Results 1 - 10 of about 257 for anderson lunt javitz "next generation intrusion detection". (0.24 secon

Did you mean: anderson lunt javits "next generation intrusion detection"

Sponsored Links Intrusion Detection Guide

www.techdirectory.ws

## Next Generation Intrusion Detection Expert System

... not include all citations): 49 Next generation intrusion detection expert system ... (context) - Javitz, Valdes - 1994 ... behavior u.. (context) -Anderson, Lunt et al ...

See your message here...

A directory of websites offering

information on intrusion detection.

citeseer.ist.psu.edu/anderson94next.html - 19k - Cached - Similar pages

Computer System Intrusion Detection: A Survey - Jones, Sielken ... ... Threat Monitoring and Surveillance (context) - Anderson - 1980 45 ... of Intrusion Detection Techniques (context) - Lunt - 1993 40 ... context) - Javitz, Valdes - 1993 ... citeseer.ist.psu.edu/mcinnes99computer.html - 23k - Cached - Similar pages [ More results from citeseer.ist.psu.edu ]

### Next-Generation Intrusion Detection System (NIDES) Home Page

... Document, Jagannathan,. Lunt, Dodd,. Anderson,. Gilham,. Jalali ... Time Intrusion Detection Expert System, Lunt,. Tamaru,. Gilham ... Jalali, Javitz. Neumann,. Valdes,. Garvey. 2/92. ...

www.sdl.sri.com/projects/nides/index5.html - 18k - Cached - Similar pages

### SRI International - System Design Laboratory Laboratory ...

... Debra Anderson led a project to adapt the NIDES ... Teresa Lunt led a project to enhance CSL's prototype ... Harold Javitz led the project, assisted by Dorothy Denning ...

www.sdl.sri.com/programs/intrusion/history.html - 24k - Cached - Similar pages [ More results from www.sdl.sri.com ]

## [PDF] Next-generation Intrusion Detection Expert System (NIDES) A ...

File Format: PDF/Adobe Acrobat - View as HTML

... 2 NIDES Final Report The Next-generation Intrusion-Detection Expert System ... Subsequent to Anderson □s study, early work ... project, led by Teresa Lunt at Sytek

www.ccss.isi.edu/papers/anderson nides.pdf - Similar pages

#### Intrusion Detection Systems Bibliography

... 1990. NIDES. Anderson, D.; Lunt, TF; Javitz, H.; Tamaru, A.; Valdes, A.: Detecting Unusaul Program Behavior Using the Stastistical Component of the Next ... www.cse.sc.edu/research/isl/mirrorIDSbibl.shtml - 28k - Cached - Similar pages

#### Studie IDS Literaturverzeichnis

... Javitz, H. and Valdes, A.: The NIDES Statistical Component: Description and Justification, SRI International, 1993. ... Lunt, T. and Anderson, D.: Next ... www.bsi.de/literat/studien/ids/doc0045.htm - 31k - Cached - Similar pages

#### [PDF] Microsoft PowerPoint - NIDES.ppt

File Format: PDF/Adobe Acrobat - View as HTML

... Program Behavior Using the Statistical Component of the Next-Generation Intrusion Detection Expert System(NIDES)", Anderson, Lunt, Javitz, Tamaru, Valdes ...

www.cs.fsu.edu/~yasinsac/group/slides/harley2.pdf - Similar pages

A high-performance network intrusion detection system ... ALJTV95 D. Anderson, T. Lunt, H. Javitz, A. Tamaru, and A. Valdes, Nextgeneration Intrusion Detection Expert System (HIDES): A Summary, SRI-CSL-95-07, SKI Int ... portal.acm.org/ citation.cfm? id=319712&di=ACM&coll=GUIDE&CFID=111111111&CFTOKEN=2222222 -Similar pages

Neil's Intrusion and Detection Bibliography

... R. Jagannathan and Teresa Lunt and Debra Anderson and Chris Dodd and Fred Gilham and Caveh Jalali and Hal Javitz and Peter Neumann and Ann Tamaru and ... www.jjtc.com/Security/bib/ids.htm - 101k - Cached - Similar pages

Did you mean to search for: anderson lunt javits "next generation intrusion detection"

Gooooooogle >

**1 2 3 4 5 6 7 8 9 10** Result Page:

anderson lunt javitz "next general

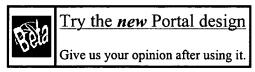
Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Solutions - Business Solutions - About Google

©2004 Google



> home > about > feedback **US Patent & Trademark Office** 



### Search Results

Search Results for: [ghosh AND schwartzbard AND schatz] Found **10** of **129,763 searched.** 

Search within Results		
	GO	> Advanced Search
> Search Heln/Tins		

Binder Sort by: Title Publication Publication Date Score Results 1 - 10 of 10 short listing

84% Intrusion detection: Mimicry attacks on host-based intrusion detection **4** systems

David Wagner , Paolo Soto

Proceedings of the 9th ACM conference on Computer and communications security November 2002

We examine several host-based anomaly detection systems and study their security against evasion attacks. First, we introduce the notion of a mimicry attack, which allows a sophisticated attacker to cloak their intrusion to avoid detection by the IDS. Then, we develop a theoretical framework for evaluating the security of an IDS against mimicry attacks. We show how to break the security of one published IDS with these methods, and we experimentally confirm the power of mimicry attacks by ...

Industrial/government track: Towards NIC-based intrusion detection M. Otey , S. Parthasarathy , A. Ghoting , G. Li , S. Narrayula , D. Panda Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining August 2003

We present and evaluate a NIC-based network intrusion detection system. Intrusion detection at the NIC makes the system potentially tamper-proof and is naturally extensible to work in a distributed setting. Simple anomaly detection and signature detection based models have been implemented on the NIC firmware, which has its own processor and memory. We empirically evaluate such systems from the perspective of quality and performance (bandwidth of acceptable messages) under varying conditions of ...

Defensive technology: Detection of injected, dynamically generated, and 80% obfuscated malicious code

Jesse C. Rabek , Roger I. Khazan , Scott M. Lewandowski , Robert K. Cunningham Proceedings of the 2003 ACM workshop on Rapid Malcode October 2003 This paper presents DOME, a host-based technique for detecting several general classes of malicious code in software executables. DOME uses static analysis to identify the locations (virtual addresses) of system calls within the software

80%

executables, and then monitors the executables at runtime to verify that every observed system call is made from a location identified using static analysis. The power of this technique is that it is simple, practical, applicable to real-world software, and high ...

**4** Intrusion detection and response: An empirical analysis of NATE:

80%

A Network Analysis of Anomalous Traffic Events Carol Taylor, Jim Alves-Foss

Proceedings of the 2002 workshop on New security paradigms September 2002 This paper presents results of an empirical analysis of NATE (Network Analysis of Anomalous Traffic Events), a lightweight, anomaly based intrusion detection tool. Previous work was based on the simulated Lincoln Labs data set. Here, we show that NATE can operate under the constraints of real data inconsistencies. In addition, new TCP sampling and distance methods are presented. Differences between real and simulated data are discussed in the course of the analysis.

5 Industry track papers: Learning nonstationary models of normal

80%

network traffic for detecting novel attacks

Matthew V. Mahoney, Philip K. Chan

Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining July 2002

Traditional intrusion detection systems (IDS) detect attacks by comparing current behavior to signatures of known attacks. One main drawback is the inability of detecting new attacks which do not have known signatures. In this paper we propose a learning algorithm that constructs models of normal behavior from attack-free network traffic. Behavior that deviates from the learned normal model signals possible novel attacks. Our IDS is unique in two respects. First, it is nonstationary, modeling pr ...

**6** -- Special-section on data-mining-for intrusion detection and threat

80%

analysis: Detection and classification of intrusions and faults using sequences of system calls

João B. D. Cabrera, Lundy Lewis, Raman K. Mehra

**ACM SIGMOD Record** December 2001

Volume 30 Issue 4

This paper investigates the use of sequences of system calls for classifying intrusions and faults induced by privileged processes in Unix. Classification is an essential capability for responding to an anomaly (attack or fault), since it gives the ability to associate appropriate responses to each anomaly type. Previous work using the well known dataset from the University of New Mexico (UNM) has demonstrated the usefulness of monitoring sequences of system calls for detecting anomalies induced ...

7 Intrusion detection: Specification-based anomaly detection: a new approach for detecting network intrusions

80%

R. Sekar , A. Gupta , J. Frullo , T. Shanbhag , A. Tiwari , H. Yang , S. Zhou Proceedings of the 9th ACM conference on Computer and communications security November 2002

Unlike signature or misuse based intrusion detection techniques, anomaly detection is capable of detecting novel attacks. However, the use of anomaly detection in practice is hampered by a high rate of false alarms. Specification-based techniques have been shown to produce a low rate of false alarms, but are not as effective as anomaly detection in detecting novel attacks, especially when it comes to network probing and denial-of-service attacks. This paper presents a new approach that combines ...

**8** Computer security: Learning temporal patterns for anomaly intrusion detection

80%

80%

Alexandr Seleznyov , Oleksiy Mazhelis

Proceedings of the 2002 ACM symposium on Applied computing March 2002 For the last decade an explosive spread of computer systems and computer networks has resulted in a society that is increasingly dependent on information stored on these systems. A computer system connected to the network is accessible from another computer in this network regardless of its geographical position. Along with providing many benefits for legitimate users this technology creates almost unlimited opportunities for malicious persons, which using software vulnerabilities may successful ...

Simple, state-based approaches to program-based anomaly detection 🔥 C. C. Michael , Anup Ghosh

ACM Transactions on Information and System Security (TISSEC) August 2002 Volume 5 Issue 3

This article describes variants of two state-based intrusion detection algorithms from Michael and Ghosh [2000] and Ghosh et al. [2000], and gives experimental results on their performance. The algorithms detect anomalies in execution audit data. One is a simply constructed finite-state machine, and the other two monitor statistical deviations from normal program behavior. The performance of these algorithms is evaluated as a function of the amount of available training data, and they are compar ...

10 A high-performance network intrusion detection system

77%

R. Sekar, Y. Guang, S. Verma, T. Shanbhag

Proceedings of the 6th ACM conference on Computer and communications **security** November 1999

In this paper we present a new approach for network intrusion detection based on concise specifications that characterize normal and abnormal network packet sequences. Our specification language is geared for a robust network intrusion detection by enforcing a strict type discipline via a combination of static and dynamic type checking. Unlike most previous approaches in network intrusion detection, our approach can easily support new network protocols as information relating to the protoco ...

#### Results 1 - 10 of 10 short listing

The ACM Portal is published by the Association for Computing Machinery. Copyright @ 2004 ACM, Inc.



News Froogle<sup>New!</sup> <u>Images</u> Groups more »

anderson lunt javitz "next generation intrusi

Search

Advanced Search Preferences

Web Results 1 - 10 of about 257 for anderson lunt javitz "next generation intrusion detection". (0.24 secon

Did you mean: anderson lunt javits "next generation intrusion detection"

Intrusion Detection Guide

www.techdirectory.ws

## Next Generation Intrusion Detection Expert System (NIDES) ...

... not include all citations): 49 Next generation intrusion detection expert system ... (context) - Javitz, Valdes - 1994 ... behavior u.. (context) -Anderson, Lunt et al ...

See your message here...

A directory of websites offering

information on intrusion detection.

Sponsored Links

citeseer.ist.psu.edu/anderson94next.html - 19k - Cached - Similar pages

Computer System Intrusion Detection: A Survey - Jones, Sielken ... ... Threat Monitoring and Surveillance (context) - Anderson - 1980 45 ... of Intrusion Detection Techniques (context) - Lunt - 1993 40 ... context) - Javitz, Valdes - 1993 ... citeseer.ist.psu.edu/mcinnes99computer.html - 23k - Cached - Similar pages [ More results from citeseer.ist.psu.edu ]

### Next-Generation Intrusion Detection System (NIDES) Home Page

... Document, Jagannathan,. Lunt, Dodd,. Anderson,. Gilham,. Jalali ... Time Intrusion Detection Expert System, Lunt,. Tamaru,. Gilham ... Jalali, Javitz. Neumann,. Valdes,.. Garvey. 2/92. ...

www.sdl.sri.com/projects/nides/index5.html - 18k - Cached - Similar pages

#### SRI International - System Design Laboratory Laboratory ...

... Debra Anderson led a project to adapt the NIDES ... Teresa Lunt led a project to enhance CSL's prototype ... Harold Javitz led the project, assisted by Dorothy Denning ...

www.sdl.sri.com/programs/intrusion/history.html - 24k - Cached - Similar pages [ More results from www.sdl.sri.com ]

## [PDF] Next-generation Intrusion Detection Expert System (NIDES) A ...

File Format: PDF/Adobe Acrobat - View as HTML

... 2 NIDES Final Report The Next-generation Intrusion-Detection Expert System ... Subsequent to Anderson □s study, early work ... project, led by Teresa Lunt at Sytek

www.ccss.isi.edu/papers/anderson\_nides.pdf - Similar pages

#### Intrusion Detection Systems Bibliography

... 1990. NIDES. Anderson, D.; Lunt, TF; Javitz, H.; Tamaru, A.; Valdes, A.: Detecting Unusaul Program Behavior Using the Stastistical Component of the Next ... www.cse.sc.edu/research/isl/mirrorlDSbibl.shtml - 28k - Cached - Similar pages

#### Studie IDS Literaturverzeichnis

... Javitz, H. and Valdes, A.: The NIDES Statistical Component: Description and Justification, SRI International, 1993. ... Lunt, T. and Anderson, D.: Next ... www.bsi.de/literat/studien/ids/doc0045.htm - 31k - Cached - Similar pages

### [PDF] Microsoft PowerPoint - NIDES.ppt

File Format: PDF/Adobe Acrobat - View as HTML

... Program Behavior Using the Statistical Component of the Next-Generation Intrusion Detection Expert System(NIDES)", Anderson, Lunt, Javitz, Tamaru, Valdes ...



A high-performance network intrusion detection system ... ALJTV95 D. Anderson, T. Lunt, H. Javitz, A. Tamaru, and A. Valdes, Nextgeneration Intrusion Detection Expert System (HIDES): A Summary, SRI-CSL-95-07, SKI Int ... portal.acm.org/ citation.cfm? id=319712&di=ACM&coll=GUIDE&CFID=11111111&CFTOKEN=2222222 -Similar pages

Neil's Intrusion and Detection Bibliography

... R. Jagannathan and Teresa Lunt and Debra Anderson and Chris Dodd and Fred Gilham and Caveh Jalali and Hal Javitz and Peter Neumann and Ann Tamaru and ... www.jjtc.com/Security/bib/ids.htm - 101k - Cached - Similar pages

Did you mean to search for: anderson lunt javits "next generation intrusion detection"

Goooooooogle ▶

1 2 3 4 5 6 7 8 9 10 Result Page:

anderson lunt javitz "next general

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Solutions - Business Solutions - About Google

©2004 Google

http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&q=anderson+lunt+javitz+... 4/2/04

IEEE HOME ! SEARCH IEEE | SHOP | WEB ACCOUNT ! CONTACT IEEE

Membership Publications/Services Standards: Confenences Careers/Jobs



三!

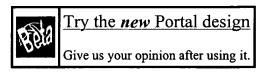
	Welcome United States Patent and Trademark Office
Help FAQ Terms IEE	E Peer Review Quick Links   ** Se
Welcome to IEEE <i>Xplores</i> O- Home O- What Can	Your search matched 2 documents.
I Access?  — Log-out	A maximum of <b>500</b> results are displayed, <b>15</b> to a page, sorted by <b>Relevance Descending</b> order.
Tables of Contents  O Journals & Wagazines	Results Key:  JNL = Journal or Magazine CNF = Conference STD = Standard
- Conference Proceedings - Standards	1 State transition analysis: a rule-based intrusion detection approach Ilgun, K.; Kemmerer, R.A.; Porras, P.A.; Software Engineering, IEEE Transactions on ,Volume: 21 , Issue: 3 , March 1 Pages: 181 - 199
Serrein  O- By Author	[Abstract] [PDF Full-Text (1864KB)] IEEE JNL
O- Basic O- Advanced	2 USTAT: a real-time intrusion detection system for UNIX  Ilgun, K.;  Research in Security and Privacy, 1993. Proceedings., 1993 IEEE Computer S
Member Services  - Join IEEE - Establish IEEE Web Account	Symposium on , 24-26 May 1993 Pages:16 - 28  [Abstract] [PDF Full-Text (892KB)] IEEE CNF
Access the IEEE Member Digital Library	

Home | Log-out | Journals | Conference Proceedings | Standards | Search by Author | Basic Search | Advanced Search | Join IEEE | Web Account | New this week | OPAC Linking Information | Your Feedback | Technical Support | Email Alerting | No Robots Please | Release Notes | IEEE Online Publications | Help | FAQ| Terms | Back to Top

Copyright © 2004 IEEE — All rights reserved



: > about : > feedback **US Patent & Trademark Office** 



### Search Results

Search Results for: [sekar AND uppuluri] Found **10** of **129,763 searched.** 

Sea	rch	within	Resu	Itc
Scal		VVILIIIII	~c≥u	ıLD

	GO	> Advanced Search
--	----	-------------------

> Search Help/Tips

Binder Publication Publication Date Score Sort by: Title

**Results 1 - 10 of 10** short listing

Safely executing untrusted code: Model-carrying code: a practical बे approach for safe execution of untrusted applications

88%

R. Sekar , V.N. Venkatakrishnan , Samik Basu , Sandeep Bhatkar , Daniel C. DuVarney Proceedings of the nineteenth ACM symposium on Operating systems principles October 2003

This paper presents a new approach called model-carrying code (MCC) for safe execution of untrusted code. At the heart of MCC is the idea that untrusted code comes equipped with a concise high-level model of its security-relevant behavior. This model helps bridge the gap between high-level security policies and low-level binary code, thereby enabling analyses which would otherwise be impractical. For instance, users can use a fully automated verification procedure to determine if the code ...

BlueBoX: A policy-driven, host-based intrusion detection system Suresh N. Chari, Pau-Chen Cheng

87%

ACM Transactions on Information and System Security (TISSEC) May 2003 Volume 6 Issue 2

Detecting attacks against systems has, in practice, largely been delegated to sensors, such as network intrustion detection systems. However, due to the inherent limitations of these systems and the increasing use of encryption in communication, intrusion detection and prevention have once again moved back to the host systems themselves. In this paper, we describe our experiences with building BlueBox, a hostbased intrusion detection system. Our approach, based on the technique of system call i ...

Mobile code: Empowering mobile code using expressive security policies 84% V. N. Venkatakrishnan , Ram Peri , R. Sekar

Proceedings of the 2002 workshop on New security paradigms September 2002 Existing approaches for mobile code security tend to take a conservative view that mobile code is inherently risky, and hence focus on confining it. Such confinement is usually achieved using access control policies that restrict mobile code from taking any action that can potentially be used to harm the host system. While such policies can be





helpful in keeping "bad applets" in check, they preclude a large number of useful applets. We therefore take an alternative view of mobile code security, ...

Data integrity: Web application security assessment by fault injection

84%

and behavior monitoring

Yao-Wen Huang , Shih-Kun Huang , Tsung-Po Lin , Chung-Hung Tsai Proceedings of the twelfth international conference on World Wide Web May 2003 As a large and complex application platform, the World Wide Web is capable of delivering a broad range of sophisticated applications. However, many Web applications go through rapid development phases with extremely short turnaround time, making it difficult to eliminate vulnerabilities. Here we analyze the design of Web application security assessment mechanisms in order to identify poor coding practices that render Web applications vulnerable to attacks such as SQL injection and cross-site scr ...

5 Intrusion detection: Specification-based anomaly detection: a new | approach for detecting network intrusions

84%

R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, S. Zhou Proceedings of the 9th ACM conference on Computer and communications security November 2002

Unlike signature or misuse based intrusion detection techniques, anomaly detection is capable of detecting novel attacks. However, the use of anomaly detection in practice is hampered by a high rate of false alarms. Specification-based techniques have been shown to produce a low rate of false alarms, but are not as effective as anomaly detection in detecting novel attacks, especially when it comes to network probing and denial-of-service attacks. This paper presents a new approach that combines ...

6 Session 1: creative mathematics: Model-Carrying Code (MCC): a new n paradigm for mobile-code security

82%

R. Sekar, C. R. Ramakrishnan, I. V. Ramakrishnan, S. A. Smolka Proceedings of the 2001 workshop on New security paradigms September 2001 A new approach for ensuring the security of mobile code is proposed. Our approach enables a mobile-code consumer to understand and formally reason about what a piece of mobile code can do; check if the actions of the code are compatible with his/her security policies; and, if so, execute the code. The compatibility-checking process is automated, but if there are conflicts, consumers have the opportunity to refine their policies, taking into account the functionality provided by the mobile code.

Enabling trusted software integrity

82%

Darko Kirovski , Milenko Drinić , Miodrag Potkonjak

Tenth international conference on architectural support for programming languages and operating systems on Proceedings of the 10th international conference on architectural support for programming languages and operating systems (ASPLOS-X) October 2002

Volume 37, 30, 36 Issue 10, 5, 5

Preventing execution of unauthorized software on a given computer plays a pivotal role in system security. The key problem is that although a program at the beginning of its execution can be verified as authentic, while running, its execution flow can be redirected to externally injected malicious code using, for example, a buffer overflow exploit. Existing techniques address this problem by trying to detect the intrusion at run-time or by formally verifying that the software is not prone to a p ...

80%



S Intrusion detection: Enhancing byte-level network intrusion detection signatures with context

Robin Sommer, Vern Paxson

Proceedings of the 10th ACM conference on Computer and communication security October 2003

Many network intrusion detection systems (NIDS) use byte sequences as signatures to detect malicious activity. While being highly efficient, they tend to suffer from a high false-positive rate. We develop the concept of *contextual signatures* as an improvement of string-based signature-matching. Rather than matching fixed strings in isolation, we augment the matching process with additional context. When designing an efficient signature engine for the NIDS bro, we provide low-level context ...

A high-performance network intrusion detection system

80%

R. Sekar , Y. Guang , S. Verma , T. Shanbhag

Proceedings of the 6th ACM conference on Computer and communications security November 1999

In this paper we present a new approach for network intrusion detection based on concise specifications that characterize normal and abnormal network packet sequences. Our specification language is geared for a robust network intrusion detection by enforcing a strict type discipline via a combination of static and dynamic type checking. Unlike most previous approaches in network intrusion detection, our approach can easily support new network protocols as information relating to the protoco ...

10 Session 4: innovative solutions: AngeL: a tool to disarm computer

77%

্রা systems

Danilo Bruschi, Emilia Rosti

Proceedings of the 2001 workshop on New security paradigms September 2001 In this paper we present a tool designed to intercept attacks at the host where they are launched so as to block them before they reach their targets. The tool works both for attacks targeted on the local host and on hosts connected to the network. In the current implementation it can detect and block more than 70 attacks as reported in the literature. The tool is based on the idea of improving the overall security of the Internet by connecting disarmed systems, i.e., hosts that cannot launch att ...

#### Results 1 - 10 of 10 short listing

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2004 ACM, Inc.



> about : > feedback : > login **US Patent & Trademark Office** 



Try the *new* Portal design

Give us your opinion after using it.

## Search Results

Search Results for: [porras AND kemmerer<AND>((Penetration State Transition Analysis: A Rule based Intrusion Detection Approach) )] Found 1 of 129,763 searched.

Search within Results		
	> Advanced Search	
> Search Help/Tips		
Sort by: Title Publication Publication Date	e Score Sinder	
Results 1 - 1 of 1 short listing		
Intrusion detection: Specification-based approach for detecting network intrusion R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Proceedings of the 9th ACM conference on security November 2002  Unlike signature or misuse based intrusion do capable of detecting novel attacks. However, is hampered by a high rate of false alarms. So shown to produce a low rate of false alarms, detection in detecting novel attacks, especial denial-of-service attacks. This paper presents	Ons Tiwari , H. Yang , S. Zhou Computer and communications  letection techniques, anomaly detection is , the use of anomaly detection in practice Specification-based techniques have been but are not as effective as anomaly lly when it comes to network probing and	80%

#### Results 1 - 1 of 1 short listing

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2004 ACM, Inc.











> about : > feedback :

**US Patent & Trademark Office** 



Try the *new* Portal design

Give us your opinion after using it.

## Search Results

Search Results for: [Penetration State Transition Analysis: A Rule based Intrusion Detection Approach]

Found 1 of 129,763 searched.

Search within Results

porras AND kemmerer



Score

> Advanced Search

> Search Help/Tips

**Publication Publication Date** Sort by: Title

Binder 🕏

Results 1 - 1 of 1 short listing

1 Intrusion detection: Specification-based anomaly detection: a new

80%

ৰী approach for detecting network intrusions

R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, S. Zhou Proceedings of the 9th ACM conference on Computer and communications security November 2002

Unlike signature or misuse based intrusion detection techniques, anomaly detection is capable of detecting novel attacks. However, the use of anomaly detection in practice is hampered by a high rate of false alarms. Specification-based techniques have been shown to produce a low rate of false alarms, but are not as effective as anomaly detection in detecting novel attacks, especially when it comes to network probing and denial-of-service attacks. This paper presents a new approach that combines ...

#### Results 1 - 1 of 1 short listing

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2004 ACM, Inc.